NETWORK AUTHENTICATION WITH SMART CHIP AND MAGNETIC STRIPE

Relation to Previous Application

This application is a continuation-in-part of application U.S. Patent Application, Serial No. 09/322,670 filed on May 28, 1999.

Technical Field:

The invention relates to methods in networked computer systems for authenticating a user to a server using a magnetic stripe card and a card reader with a smart chip connected to or embedded in a user device such as a computer or cellular telephone.

Background of the Invention:

Many forms of plastic cards have magnetic stripes that contain the cardholder's personal information, *e.g.*, name and card account number. There are readers for reading the magnetic stripes at many retail point-of-sale locations. Debit cards can be used at these locations by swiping the card through the reader and entering a personal identification number (PIN) into the reader's keypad. Adequate authentication of the user is achieved by a secure communications connection between the reader and a remote computer/server and by the cardholder possessing a debit card that can be read by the reader and knowing the PIN associated with the card.

For transactions on unsecure networks such as the internet, the above-described secure authentication features are not available. There is no adequately secure communications connection between a card reader that is connected to the user's host computer and the remote computer/server.

Various companies, including IBM, Hewlett-Packard, Intel, and Wave have proposed solving this problem by including a "smart chip" in each personal computer for secure authentication. The smart chip stores or creates on command a unique, encrypted identification code that cannot be read but can be used to prove the identification of the chip to a remote computer/server across a communications line. Thus, proper decryption of this code by the server provides a secure identification of the computer. Presumably, the owner of the host computer with the smart chip can

be held responsible for its use. Entry of a PIN at a keyboard connected to the host computer may also be required. With the ability to prove which host computer placed a communication for a transaction and that a particular PIN was used, adequate secure authentication will be achieved for many network transactions.

Other companies have proposed the use of smart cards placed in a smart-card reader at each host computer for secure authentication. Each smart card includes a smart chip as described above. The smart card is guarded by its owner like a key. The person who possesses the smart card is presumed to be its proper owner. Entry of a PIN at a keyboard connected to the host computer to which the smart card reader is connected can also be required. With the ability to prove which smart card was used for a transaction and that the PIN associated with the smart card was also used, adequate secure authentication will be achieved for many network transactions.

SUMMARY OF THE INVENTION

The invention is a method for using a device that incorporates a mag-stripe card reader head with a smart chip and can be connected to a computer network such as the internet. The device includes a slot for swiping a mag-stripe card, a read head within the slot, and a secure identity circuit for authentication (smart chip). For purposes of this discussion, a smart chip (authentication circuit) is a circuit that can perform authentication to a remote server across a network by confirming a unique identification to the remote server without revealing to the local computer or any intervening device in the communications link enough information that, if captured, can be used to imitate the smart chip. Such chips are well known. They generally work by using a secret key to encrypt a piece of information. If the appropriate decryption key successfully decrypts the information, the identity is authenticated.

The authentication circuit (smart chip) provides a unique identity of the device and the person to whom the smart chip was issued is kept in a database. Although the mag-stripe card can be duplicated or imitated, unlike the smart chip, and is therefore less secure than the smart chip, requiring the use of a mag-stripe card with certain information which matches information contained within a database as well as the smart chip increases the confidence of authentication. Therefore, such a device provides additional security to a transaction on an unsecure network such as

the internet because the user was required to possess both the magnetic stripe card with appropriate information and a smart chip that authenticates to the server, thereby increasing the security of authentication.

For still greater security of authentication, a personal identification number (PIN) is also required. The PIN may be associated either with the mag-stripe card or with the smart chip or be a single PIN which is associated with both of them. The PIN may be verified by the smart chip or it may be transmitted to the server for verification, preferably using encryption by the smart chip before it is transmitted. The PIN may be entered on a keyboard of a personal computer to which the device is connected or, for better security, on a keypad on the device with the smart chip.

The reader device with the smart chip may be used by a merchant to authenticate himself to a financial institution using the smart chip and a PIN. The merchant may then swipe a payment card, such as a credit card or debit card, from a customer to perform a card present financial transaction. If the entry of a PIN is required of the customer, the customer can enter a second PIN on the keypad. When used for this purpose, the merchant will have entered a PIN to authenticate the identity of the merchant and the customer will also have entered a PIN to authenticate the identity of the customer.

If the user device is configured to work with several different mag-stripe cards, each can require a different PIN. Information from the mag-stripe card is passed to the smart chip which then determines which PIN is required based on that information and based on information securely stored in the smart chip's memory. Also, the information read from the magnetic stripe card can be used to verify that an appropriate card has been swiped. If the information read from the card does not match processing requirements securely stored in the smart chip, the required authentication will fail.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows the invented method in a preferred embodiment.

Figure 2 shows a variation of the invented method where data from the mag-stripe is verified on a server.

Figure 3 shows an elaboration of the method for use in payment card transactions.

Figure 4 is a side plan view of a card reader with smart chip.

Figure 5 is a block diagram of the circuitry for the card reader of Figure 4.

Figure 6 is a top plan view of a cellular telephone that includes a smart chip and card reader.

Figure 7 is a front perspective view of a computer system to which is connected the card reader of Figure 4.

DETAILED DESCRIPTION OF THE INVENTION

Each card reader is uniquely identified by a smart chip, which may be on a removable card, and each smart chip is associated with a respective owner through the unique identification. The unique identification code of the smart chip is registered on a remote central computer/server in association with accurate identification of the owner to whom the smart chip was issued. Using a secure PIN, the smart chip owner can access the functions of the smart chip. When a cardholder places a mag-stripe card in the reader, the name or other identification is read from the card and is compared with an identification on the central computer/server associated with the unique identification code stored in or generated by the smart chip. If the name and code do not match, then the transaction may be disallowed for inadequate authentication. By this process, two hardware items are required to authenticate the user: a mag-stripe card containing certain information and a smart chip with a secure authentication feature proving a certain identification. Requiring both together provides a more secure authentication than requiring either alone. For further security, a PIN may also be required.

The card reader is preferably portable and easily connected to or disconnected from the cardholder's computer or any other host computer.. This allows the cardholder to easily guard his/her possession of the reader and to permit others to use his/her computer without a security risk. Alternatively, the smart chip may be removable to achieve the same security. Unlike prior art smart card systems, however, possession of only the smart-card reader and knowledge of a PIN is not enough to establish authentication. A mag-stripe card encoded with either a name that matches the name of the cardholder to which the reader was issued or a number that is on the authorized list is also required. Therefore, because the mag-

stripe card reader with smart chip is like a key, it is aptly described as a card reader with an electronic key.

To perform the authentication, the smart chip encrypts the identification code and magnetic-stripe information according to conventional encryption techniques. Alternatively, the identification code may be stored in encrypted form on the smart chip or the information may be stored in encrypted form on the magnetic stripe for processing by the smart chip before being sent to the server. In such a case, the microcontroller does not alter the code or the magnetic-stripe information before sending it to the remote computer/server.

Then, the remote computer/server determines whether the cardholder identified by the magnetic-stripe information is authorized to use the card reader having a smart chip with the unique identification code. Typically, the remote computer/server stores the information for the cardholder who is authorized to use the particular card reader. Therefore, if the magnetic-stripe information corresponds to cardholder information stored for the unique code, then the remote computer/server allows the transaction to proceed. If, however, the magnetic-stripe information does not correspond to the cardholder information stored for the unique identification code, then the remote computer/server cancels the transaction.

Methods Performed by the User Device and Servers

Figure 1 shows the preferred method for using a card with a magnetic stripe and a smart chip to authenticate a user. In step **101**, data is read from the magnetic stripe on the card by the magnetic stripe reader head. The data is processed in the local device, step **102**. The functions of the local device may be performed in the smart chip or, for those functions which do not require the security of a smart chip, in an auxiliary processor. The data read from a card is verified, either by merely confirming that it appears to be complete and in the correct format or by using a secure storage feature of the smart chip to determine that the data read from the magnetic stripe, such as a user name or account number, matches data securely stored in the smart chip.

In step **102**, information which is a function of the data read from the magnetic stripe, f(data), is stored in the smart chip or in an auxiliary memory. What is stored can be a portion of the original data or a hash of part of the original data or a

signature generated from part of the original data or an encryption of the data or any other information which is derived from the data and varies as a function of the data contents.

Once f(data) has been stored, the process proceeds to step **103**. In step **103**, the user enters a personal identification number (PIN) at a keyboard. The keyboard is preferably not connected to a personal computer because they are unsecure and can be monitored by unauthorized software to capture the user's personal identification number. The keyboard is preferably located on a device containing the smart chip which is, in turn, connected to the personal computer such that the PIN is never transmitted to the personal computer.

In step **104**, the PIN is verified. This can be accomplished in many ways. The preferred method is to use the well known PIN function of a smart chip. Alternatively, the PIN can be encrypted by an encryption function of the smart chip or a separate encryption circuit and transmitted to a remote server for verification. The PIN can be a PIN which is associated with the card or a PIN which is associated with the smart chip or a single PIN which is associated with both of them. If the information in the smart chip is configured to work with several mag-stripe cards, the PIN verification can be done in the smart chip even though any of several different PINs are verifiable.

Once the PIN is verified, the process proceeds to step **105**. In step **105**, information to be processed is received by the local device. If the authentication system is being used for a payment transaction, the information to be processed will be the details of the payment transaction specifying a dollar amount or a party to be paid or any other appropriate information. If the purpose of the authentication is to establish a digital signature which can not be repudiated, the information to be processed will consist of the document to be signed with the digital signature. If the purpose of the authentication is to allow an authorized person to make use of a secure network, the information to be processed will typically be a user name or a password for the network.

In step **106**, the information derived from the mag-stripe, f(data), is combined with information to be processed and the smart chip is used to encrypt or sign the combined information with a key that a recipient can decrypt or verify.

In step **107**, the signed or encrypted combined information is transmitted on an unsecure network or placed in a storage device for physical transmission to a recipient.

In step **108**, the recipient identifies the appropriate key to use for decrypting the signature or the entire combined information based on an identification of the sender. The identification of the sender can be determined from an identification of the smart chip or data from the mag-stripe card. The recipient then uses the key to decrypt the signature or combined information. If the decryption is successful, this authenticates the identification of the smart chip that was used and reveals f(data) derived from magnetic stripe information on the card which can then be compared to records in a database to verify that the correct card (or a counterfeit thereof) was present.

In the process just described, the user was authenticated based on (1) possession of a magnetic stripe card with appropriate data and (2) possession of a smart chip with an appropriate encryption key and (3) knowledge of an appropriate personal identification number (PIN).

Figure 2 illustrates some variations on the method shown in Figure 1. One of the variations is that a personal identification number is not required. Another variation is that the verification of data read from the mag-stripe on the card is done on a remote server before the smart chip is used to encrypt or sign information such that when the information is decrypted authentication of the smart chip is established. The server that verifies the mag-stripe data before the process is allowed to proceed may be a different server from the server that receives the information to be processed.

In step **111**, data is read from the mag-stripe on the card. In step **112**, this data is encrypted and forwarded to a server via an unsecure network. In step **113**, the mag-stripe information is decrypted to verify that the correct mag-stripe card has been read. Of course, for the essential purposes of the invented method, the mag-stripe data need not be encrypted before being forwarded to the server for verification. However, to minimize security risk, it is preferable to encrypt the information before transmission on the unsecure network. If the information on the card is verified, the process, on both the local device and on the server, then proceeds to the next step.

In step **114**, information to be processed is received at the local device with a smart chip. At step **115**, the information or a part of the information or a hash of the information is encrypted or signed and transmitted on the network. At step **116**, the server is ready to receive the encrypted or signed information because it has already verified the data from the mag-stripe or has received a message from another server that this step was accomplished successfully. It then decrypts the information to verify that it was encrypted with a key contained within the appropriate smart chip. The user has now been authenticated based on both the smart chip and the data from the mag-stripe. In step **117**, the information which has been authenticated is forwarded to recipients who rely on the authentication.

Figure 3 shows how the authentication based on a smart chip and a mag-stripe card is performed in the context of payment card transactions. A variation illustrated in Figure 3 is a step of mutual authentication between the user device and an authentication server.

In step **121**, a personal account number (PAN) is read from the magnetic stripe on a payment card, which may be a credit card or debit card or ATM card. In step **122**, the PAN is verified by the smart chip. The smart chip contains a copy of the PAN or data which is derived from the PAN, f(PAN), in its secure memory where it cannot be extracted from the smart chip. For the verification process, the PAN read from the mag-stripe card is loaded into the smart chip which performs a routine to compare it to the PAN or f(PAN) within its secure memory. The smart chip then returns a verification that the PAN is correct or a denial that it is not correct. Then, somewhere in the user device, in the smart chip or in other memory, information which is a function of the PAN, f(PAN), is stored. If the PAN is verified, the process proceeds to the next step. If not, the process is aborted. The step of verifying the PAN can be omitted to allow any card to be used with the user device as discussed below.

In step **123**, a PIN entered by a user is received from the keyboard. As discussed above, the keyboard is preferably connected to the user device but not to a local personal computer. In step **124**, the PIN is verified by the smart chip. If the PIN is verified, the process proceeds to the next step. If it is not, the process is aborted.

In step **125**, the smart chip in the user device initiates a communication to an authentication server across a network. At this point, the PAN has been verified and the PIN has been verified. Now the authentication server verifies the identification of the smart chip using any of several well established smart chip authentication procedures, step **126**. The authentication may be one sided, as just described, from the user device to the server. Preferably, the server also authenticates itself to the user device by sending to the user device an encrypted nonce which only the user device with a key contained within secure memory in the smart chip can decrypt. If the user device properly authenticates itself to the server and the server properly authenticates itself to the user device, the user device will then proceed to the next step.

At this point, the user has been authenticated by possession of a positively identified smart chip, possession of a card with a magnetic stripe (or a counterfeit thereof) and knowledge of a personal identification number. As mentioned above, the requirement of the PIN can be omitted. If any one of these three required elements has failed, the process is aborted.

In step **127**, transaction data is received by the user device. This will typically be a dollar amount and an identification of a merchant to be paid. Because the personal account number will be required for subsequent processing of the transaction, f(PAN) is combined with the transaction data and the two are encrypted or signed using the smart chip, step **128**. The encrypted or signed data is transmitted across an unsecure network to a recipient.

At step **129**, the recipient computer decrypts the encrypted or signed data. If decryption is successful, this verifies that a particular key was used which key is contained only in a certain smart chip, thereby authenticating that the particular smart chip was used. To determine which key to use for decryption, the owner of the smart chip is verified based upon the personal account number which was transmitted in one form or another as f(PAN).

As an alternative embodiment, instead of using f(PAN) to look up the key to use for decryption, other unencrypted information identifying the smart chip can be sent along with the transaction data and f(PAN). This other information can then be used to find the key for decrypting a message encrypted with that smart chip. In this embodiment, the mag-stripe card that is used in step **121** can be a card that does

not belong to the person who owns the smart chip used for encryption in step **128**. For example, the reader with smart chip can be a merchant who wishes to accept a credit card or a debit card for payment. In this case, in addition to the smart chip owner entering a PIN in step **123,** the card holder can be required to enter a PIN for the cardholder for verification by a server. If the card was a credit card, the fact that f(PAN) was derived from data read from the card provides a verification that the card was present. If the card is a debit card, the card owner has entered the appropriate PIN which is then encrypted along with f(PAN) in step **128** and forwarded to the recipient for verification of the PIN entered by the cardholder.

If additional security is desired in any of the above described methods or variations, the server can transmit to the user device a challenge seeking a response that only an authentic user would know, such as date of birth, mother's maiden name, social security number, PIN, etc. The challenge can be presented on a screen display at the user's location, typically a personal computer or cell phone. The response entered by the user can be sent, with or without encryption, to the server as an additional authentication step.

In addition to the suggested uses for payment card transactions, the invented method can be used for additional security for digital signatures. By requiring the party making the signature to possess both the proper smart chip and the proper card with a magnetic stripe, it becomes more difficult for the owner of these two devices to later repudiate his signature and claim that he was impersonated. This can have particular value for parties who wish to guarantee signatures of others in transactions such as stock transfer transactions. In these situations, the company responsible for making stock transfers relies on a trusted party to guarantee the signature of the transferor who is someone that the guarantor knows or has meet in person to satisfy himself on identification. The guarantor then needs to apply his own digital signature so that the transaction information can be immediately transferred by a network for execution. By requiring the guarantor to possess both the magnetic stripe card with appropriate data and a smart chip with an appropriate securely stored encryption key, the stock transfer company can be confident that they are dealing with the guarantor and not an impersonator.

User Device Hardware Description

The mag-stripe card reader with smart chip may be embodied in a PCMCIA card for insertion into a PCMCIA slot, in an external card reader that plugs into a serial or parallel port or keyboard port such as the Innovonics device (Figure 11 of US Patent 5,815,577), or in a device which is mounted in the case of a personal host computer much like a disk drive or CD-ROM drive. Because the reader includes a smart chip, which may be removable, the smart chip may be used for other familiar smart chip functions such as digital signatures or storing electronic cash for micro-payments. The mag-stripe reader with smart chip may be coupled to a computer system or to a web TV system by any of the familiar methods: serial port, parallel port, keyboard port, USB port, infrared link, PCMCIA slot, or simulation of a floppy disk in a disk drive as disclosed in US patent application serial number 09/322,669 by one of the same inventors.

The mag-stripe card reader with smart chip may be incorporated into another portable device such as a cellular telephone (Figure 6) or personal digital assistant (PDA). When incorporated into a cellular telephone, a credit card or debit card may be used to charge a telephone call or remotely authorize a charge to the account for any other reason, or the owner can download cash (telephone usage credits) into the smart chip and then give the telephone to another to use with the stored credits as a limit on the amount of telephone charges that can be incurred. Similarly, when incorporated into a PDA, it may be used with the PDA's communication features.

Figure 4 is a side plan view of a card reader 10 according to an embodiment of the invention. The reader 10 includes a housing 12 having a slot 14 for receiving a card 16 having a magnetic stripe 18. The slot 14 provides adequate clearance for receiving the card but a tight enough fit to ensure that the magnetic stripe 18 is properly aligned for reading. A conventional magnetic read head 20 reads the information stored on the magnetic stripe 18 as the card 16 is inserted into the slot 14. An optional and conventional sensor 22 senses whether the card is present within the slot 14. A smart chip 24, which may be removable such as by mounting on a smart card or on a SIM, contains a unique code that identifies the card reader 10. A cable 26 allows communication to a host computer such as a personal computer, or the card reader 10 may be wireless, and thus include a radio or infrared transmitter instead of the cable 26. A light-emitting-diode (LED) array 28 or other display indicates the status of the card-reader 10. An optional keyboard, shown as

component 60 in Figure 7, allows the user to enter a personal identification number (PIN). With the keyboard and a removable smart chip on a card placed in smart card slot 62 in Figure 7, this device is essentially the same as shown in Figure 11 of US Patent 5,815,577 to Innovonics.

The smart chip 24 may be programmed for authentication via dual key (public/private) encryption such as for use with the secure electronic transactions (SET) protocol. Alternatively, the smart chip 24 may include electronic-key circuitry that is capable of authentication by securely encrypting a unique identifier and transmitting it to a remote computer/server such as with DES encryption or another encryption protocol.

Figure 5 is a schematic block diagram of a circuit 30 for the card reader 10 of Figure 4. The circuit 30 includes the smart chip 24 and the LED 28. In addition, the circuit 30 includes optional card detection/retention circuitry 32. In one embodiment, the circuitry 32 includes the card sensor 22 (Figure 4) and monitors whether the card 16 (Figure 4) is inserted within the slot 14 or not. In another embodiment, the circuitry 32 includes conventional hardware for retaining the card 16 within the slot 14 until a transaction is complete. Additionally, if the user enters a wrong PIN number for more than a predetermined number of times or performs some other incorrect act, the circuitry 32 may permanently retain the inserted card on the basis that the user is not authorized to possess it. Magnetic-stripe read circuitry 34 includes the read head 20 (Figure 4) and reads the magnetically encoded data from the magnetic stripe 18 and converts it into a digital read signal. A microcontroller 36 is coupled to the smart chip 24, the LED circuit 28, the detection circuit 32, and the read circuitry 34. In one embodiment, the microcontroller 36 includes a processor, buffers, memory, and other peripheral circuits. Alternatively, the microcontroller functions may be preformed by a microcontroller in the smart chip or by a programmable logic array or other logic circuit.

Referring to Figures 4 and 5, in operation, a cardholder inserts the card 16 into the slot 14 of the card reader 10 after the LED array 28 indicates that the reader 10 is ready to accept the card 16. As the magnetic stripe 18 moves by the read head 20, the head 20 senses the magnetically encoded information on the stripe 18 and converts this information into electrical signals. The read circuitry 34 then converts these electrical signals into a digital signal that represents the stored

information and provides this digital signal to the microcontroller 36. After the microcontroller 36 receives this stored information, it causes the LED to indicate successful reading. Additionally, the sensor 22 generates a signal indicating that the card 16 has been inserted into the slot 14, and the circuitry 32 provides this signal to the microcontroller 36.

Next, the microcontroller 36 obtains the unique identification code from the smart chip 24, which is preferably generated by encryption of data received from an external source, and provides this unique code and the information read from the magnetic stripe 18 to a remote computer/server via the host computer to which the card reader 10 is connected.

The microcontroller may also send confirmation to the remote computer/server that the card 16 is inserted within the slot 14, *i.e.*, that the card 16 has not been removed from the slot 14 since the magnetic-stripe information has been read. The remote computer/server may cancel the requested transaction if the card 16 is removed from the slot 14 before the transaction is complete. The circuitry 32 provides information to the microcontroller 36 as to the relative position of the card 16 with respect to the slot 14. In one embodiment, the card sensor 22 detects when the cardholder removes the card 16 from the slot 14, and the circuitry 32 notifies the microcontroller 36. If the transaction is not completed, then the microcontroller 36 notifies the remote computer/server of the premature card removal, and the remote computer/server may cancel the transaction in response to this notification. Alternatively, the remote computer/server may periodically poll the microcontroller 36, which notifies the remote computer/server of the card position (inserted or removed) with respect to the slot 14.

Still referring to Figures 4 and 5, the card sensor 22 and the card detection circuitry 32 are omitted from the card reader 10 in another embodiment of the invention. In this embodiment, the microcontroller 36 determines that the card 16 is inserted into the slot 14 in response to receiving the magnetic-stripe information from the read circuitry 34 as the cardholder inserts the card 16 into the slot 14. Likewise, the microcontroller 36 determines that the card 16 is removed from the slot 14 in response to receiving the magnetic-stripe information as the cardholder removes the card 16 from the slot 14. Therefore, in one embodiment, the microcontroller 36 receives the magnetic-stripe information as the cardholder inserts the card 16 into

the slot 14 and sets a corresponding flag. As long as the microcontroller 36 does not re-receive this information, it determines that the card 16 is present within the slot 14 and does not reset the flag. But once the microcontroller 36 receives the magnetic-strip information again, it determines that the cardholder is removing or has removed the card 16 from the slot 14 and thus resets the flag. The microcontroller 36 may then notify the remote computer/server of the card's removal as discussed above.

Figure 6 is front plan view of a cellular telephone 40, which includes a card reader according to an embodiment of the invention. The telephone 40 includes a case 42 and a card slot 44 formed therein. The telephone 40 also includes the smart chip 24, which might be removable by mounting on a SIM chip such as is commonly used in cellular telephones, and the read head 20, and may include the card sensor 22, of Figure 4 and the circuitry 30 of Figure 5. Alternatively, the telephone 40 may omit the sensor 22 and use the microcontroller 36 to determine the card position with respect to the slot 44 as described above. The slot 44 has a stop 46 to hold the card in place while the transaction is taking place. The telephone 40 transmits the unique identification code from the smart chip, information read from the magnetic stripe 18 of the card 16 (Figure 4), and other transaction information via an antenna 48 and cellular network (not shown) to the remote computer/server.

Figure 7 is a front view of a computer system 50, which includes the card reader 10 according to an embodiment of the invention with a slot 14 for the mag-stripe card. The system 50 includes a computer 52 and a monitor 54, keyboard 56, and mouse 58 connected to the computer 52. The keypad 60 on the card reader is shown, as well as the slot 62 for removing the smart chip which is mounted on a smart card. This embodiment is essentially the same as shown in Figure 11 of US Patent 5,815,577 to Innovonics. Alternatively, the card reader with smart chip may be incorporated into the personal computer.

From the foregoing it will be appreciated that, although specific embodiments of the invention have been described herein for purposes of illustration, various modifications may be made without deviating from the spirit and scope of the invention which is defined in the following claims.